Projet de PSSI générique pour les établissements d'enseignement supérieur

Dominique Launay
Comité Réseau des Universités
Centre de Ressources Informatiques, Campus de Beaulieu, CS 74205 , 35042 Rennes Cedex

Jean-Paul Le Guigner
Comité Réseau des Universités
Centre de Ressources Informatiques, Campus de Beaulieu, CS 74205 , 35042 Rennes Cedex

Résumé

Un groupe de travail, nommé SDS-SUP, a été constitué en 2005 à la demande de la Conférence des Présidents d'Université (CPU), la Direction de la Recherche (DR), la Direction de l'Enseignement Supérieur (DES) et le Haut Fonctionnaire de Défense et de Sécurité (HFDS) du ministère en charge de l'enseignement supérieur et la recherche, afin d'accompagner les EES dans leur démarche de gestion de la sécurité des systèmes d'information et plus spécifiquement de mise en application du SDSSI (Schéma Directeur de la Sécurité des Systèmes d'Information).
La mission de ce groupe, animé par la FSSI (Fonctionnaire SSI, service du HFDS) et le Comité Réseau des Universités (CRU), est de constituer un référentiel documentaire dans le domaine de la sécurité des systèmes d'information, notamment concernant les meilleures pratiques.
À ce titre, un programme de travail a été défini dans lequel a été retenu le projet de fourniture d'une Politique de Sécurité des Systèmes d'Information (PSSI) générique pour les établissements d'enseignement supérieur et recherche associée à une boîte à outils permettant sa déclinaison dans chaque établissement.
Ce projet, suivi par le sous groupe GT-PSSI, passe par une procédure d'appel d'offre à laquelle participent sept établissements d'enseignement supérieur dans le cadre d'un groupement d'achat.
De l'étude qui sera menée dans chacun de ces établissements doit ressortir un ensemble documentaire constituant une PSSI générique en plusieurs volets.

Mots clefs

SMSI, EBIOS, PSSI, ISO27002, ISO27001, ISO27005, appréciation du risque

1 Préoccupations initiales

1.1 Historique

1.1.1 L'organisation de la SSI dans l'Enseignement Supérieur et la Recherche

Le déploiement de RENATER et des réseaux régionaux entre 1991 et 1993 entrainera une généralisation progressive du raccordement des sites enseignement supérieur et recherche et par conséquent la propagation des protocoles TCP/IP vers tous les réseaux de campus, exposant ainsi le parc informatique des établissements aux risques déjà présents à l'époque d'intrusion, de virus,

Cette préoccupation de protection des sites et de réaction en cas d'incident, conduira les membres du GIP RENATER a créer, en mi-93, le CERT RENATER avec pour mission, la diffusion des avis de sécurité, l'aide aux sites en cas d'incident et le lien avec ses homologues étrangers.

En accompagnement de cette décision une charte d'utilisation du réseau RENATER sera publiée, revue en 1996 et toujours en application à l'heure actuelle, ce qui prouve sa pertinence.

Début 1994, conscient de la nécessité de prolonger ces actions du GIP RENATER au niveau des établissements, le Ministère, s'appuyant sur le CRU, propose la mise en place du réseau des « Correspondants de Sécurité » et contribue au montage de sessions de formations lourdes afin d'élever le niveau des compétences des correspondants désignés. L'UREC-CNRS contribuera activement à ces formations assurant ainsi une cohérence d'action MESR-CNRS.

Nous parlions de « Sécurité Informatique », de « Sécurité des Systèmes Informatiques » et puis de « Sécurité des Systèmes d'Information ».

Début 98, le réseau des « Correspondants de Sécurité » verra ses mission consolidées et son existence mieux formalisée pour devenir le réseau des RSSI (Responsable de la Sécurité des Systèmes d'Information). Si cette ossature d'organisation n'a pas changé depuis cette époque, les préoccupations, la responsabilité ainsi que le profil des activités des RSSI ont quant à eux évolué.

1.1.2 De la « Sécurité Informatique » au SDSSI, à la PSSI

Les prérogatives et les actions des Correspondants Sécurité, puis des RSSI, jusqu'au début des années 2000 concernaient plus particulièrement le domaine technique, nous avions à faire de la sécurité informatique et de la sécurité réseau appliquées aux systèmes, logiciels, matériels. Ce propos doit cependant être pris avec précaution tant peuvent être différentes les approches des établissements.

En début 2002, au niveau du Ministère, débutent les travaux du SDS (Schéma Directeur de la Sécurité) qui aboutiront à la publication, en 2005, du SDSSI (Schéma Directeur de la Sécurité des Systèmes d'Information). L'Enseignement Supérieur y contribuera en s'appuyant sur le groupe SDS-SUP. Les journées RSSI de mars 2003 évoqueront ces réflexions, mais il ne sera toujours pas question de PSSI, terme qui n'était pas encore intégré dans la prose du futur SDSSI.

Ce n'est que début 2004, avec les premiers travaux du groupe CAPSEC (CNRS) que la problématique PSSI émergera et s'installera de façon durable dans les esprits comme étant un objectif primordial qu'il faut atteindre. CAPSEC publie ses résultats courant 2005.

Le CNRS publie en fin 2006 un document intitulé « Politique de Sécurité des Systèmes d'Information » qui comprend une partie stratégique sur les grandes orientations en matière SSI au CNRS ainsi que des préconisations pour une démarche de création de PSSI d'entités.

Le CNRS porte aujourd'hui ses efforts sur la déclinaison des référentiels nationaux en documents servant de PSSI de laboratoires, avec pour finalité d'y intégrer les éléments qui leur sont spécifiques après analyse de risques locale.

1.1.3 Que comporte une PSSI ?

Un texte stratégique

Une Politique de Sécurité des Systèmes d'Information, comme son nom l'indique c'est un document de politique et comme toute politique il comporte un texte stratégique motivant un ensemble de règles qui suivent et qui matérialisent la mise en application concrète des objectifs stratégiques. Il identifie les objectifs majeurs que se fixe l'établissement en terme de protection de l'information, de la sécurité des SI, du respect des aspects légaux et règlementaire, de la protection des personnes, etc.

Ce texte doit prendre en considération les enjeux liés aux missions, aux métiers et au contexte de l'établissement ainsi que ses obligations vis à vis des tutelles, des partenaires, des personnels, etc. Il doit prendre en compte la réalité, ne pas la brusquer, appréhender à leur juste valeur les « obligations économiques » et ne pas oublier que nous vivons dans un « monde ouvert ».

Un référentiel documentaire auquel se conformer

Une PSSI doit obligatoirement s'inscrire dans un existant: textes juridiques ou règlementaires, obligations vis à vis des tutelles, textes contractuels vis à vis des partenaires, etc. A noter qu'une bonne partie de ces textes sont identiques quelques soient les établissements.

Un ensemble de règles à appliquer et respecter

La PSSI inclus des listes de règles qu'il s'agit de mettre en œuvre et de faire respecter. Ces règles résultent d'un travail d'analyse des risques prenant en compte les menaces potentielles et les objectifs de protection que l'établissement s'est fixés.

Suivant les établissements ces règles peuvent être différentes, mais un dénominateur commun de taille respectable existe.

Mais pour que ces règles soient applicables et restent en phase avec les besoins de l'établissement, elles doivent être régulièrement confrontées aux faits constatés dans l'établissement (avancées technologiques, incidents survenus...). Dans le cas contraire, ce document risque de devenir un classeur prenant la poussière dans le bureau du RSSI. Ce processus de révision est formalisé dans ce que la norme ISO27001 appelle un PDCA (Plan : planifier, Do : faire, Check : vérifier, Act : agir).

Il est donc nécessaire de vérifier régulièrement l'observation ou non de ces règles et, dans le cas où elles ne seraient pas observées, d'en évaluer la pertinence (trop contraignantes au regard du service à rendre ou mal formulées par exemple). À contrario, un incident de sécurité peut révéler l'inefficacité d'une règle pourtant respectée (la règle n'a pas empêché la perte de données par exemple). Ces révisions peuvent être programmées périodiquement (revue d'une partie spécifique de la PSSI) ou ponctuellement, à l'occasion d'un ajout de service ou de modification profonde d'architecture (mutualisation ou au contraire décentralisation).

1.1.4 Du côté Enseignement supérieur, avant les travaux PSSI

En ce qui concerne le monde Enseignement Supérieur, la prise en compte d'une réflexion sur le volet PSSI verra le jour progressivement et prendra de l'importance en 2005 avec la création du groupe de travail GT-PSSI avec au début un objectif humble d'échange de compétences en vue d'aider les établissements dans leur démarche d'élaboration de PSSI. Les efforts portèrent sur les domaines de la sensibilisation et de l'information, mais ne suffirent pas pour faire décoller les projets de PSSI d'établissements. Ce constat fera qu'en fin 2007, le S3IT inclura dans son plan d'action le projet « PSSI générique » pour l'Enseignement supérieur, décision qui aboutira au financement et au démarrage du projet en début 2009 sous la responsabilité du groupe GT-PSSI.

La lenteur observée pour le déploiement de PSSI, n'a pas signifié pour autant une absence d'action dans le domaine SSI. Diverses initiatives et mesures prises par ailleurs ont permis d'élever le niveau de sécurité des systèmes d'information et des infrastructures. Parmi celles qui méritent d'être citées :

- la publication du SDSSI en 2005 accompagnée par une série de sessions de sensibilisation des décideurs en académies ;
- la fourniture de certificats électroniques (certificats de personnes et certificats serveurs), via l'IGC pilote du CRU entre 2003 et fin 2008, ayant un succès raisonnable pour les certificats serveurs, bien plus maigre pour les certificats de personnes ;
- la fourniture de certificats serveurs reconnus dans les navigateurs basée sur le service SCS de 2006 à 2009, opération ayant connu un vrai succès et poursuivi ;
- la mise en chantier de la Fédération d'Identités pilote du CRU en 2004 qui deviendra en 2009 la Fédération Éducation-Recherche ;
- les publications de deux documents importants de recommandations : le guide Informatique et Libertés (partenariat CPU/CNIL), et la politique de gestion des traces validés par la CNIL en novembre 2008 ;
- Les éléments de recommandations pour la sécurisation des réseaux sans fil et en complément le service eduroam, ayant démarré en phase pilote en fin 2004 ;
- la mise à disposition de l'Intranet d'information pour les aspects juridiques et d'un guichet unique de réponse aux questions des établissements.

1.2 Démarrage du groupe de travail GT-PSSI

En 2005, se met en place le groupe GT-PSSI, il est constitué principalement de RSSI d'établissements dont la réflexion sur la nécessité de mettre en place une PSSI est déjà avancée. La première réunion, en comité restreint (5 personnes), a été l'occasion d'aborder les orientations vers lesquelles le groupe de travail devait orienter ses réflexions. La méthode d'analyse de risque la plus connue dans notre environnement est la méthode EBIOS. Cette méthode est exhaustive. Le paramètre sur lequel on peut jouer est la taille du périmètre du système étudié. Car il est bien évident que plus les éléments sur lesquels on va baser l'analyse sont nombreux, plus la matrice des vulnérabilités et méthodes d'attaques sur ces éléments va être complexe et plus l'analyse devient lourde à mener à son terme surtout à l'échelle d'un établissement complexe tel qu'une université.

De plus, se retrouver dans la jungle des référentiels, normes, méthodes et leur articulation n'est pas chose évidente au premier abord.

Cette première réunion a alors été l'occasion de se demander si on ne pouvait simplifier le travail au maximum pour les établissements. Les questions suivantes étaient posées en préambule de cette réunion :

- Peut-on faciliter la tâche des établissements en leur fournissant un questionnaire EBIOS allégé ou doivent-ils dérouler complètement la méthode ?
- Une PSSI type pour les établissements d'enseignement supérieur peut-elle être envisagée ? Si oui, quelle méthode pour l'élaborer ?
- Doit-on faire l'économie de méthodes, certes longues à dérouler, mais qui permettent d'impliquer entre autre les directions des établissements ?
- À quel degré peut-on réutiliser les travaux du groupe de travail CAPSEC (CNRS) dans le cadre de nos établissement ?

Nous avions considéré comme préalable implicite pour une PSSI l'utilisation de la méthode PSSI de la DCSSI utilisée conjointement avec la méthode EBIOS.

Dès la deuxième réunion, le groupe de travail s'est étoffé avec des membres du CNRS et du groupe CAPSEC. Le CNRS ayant déjà sa PSSI et le groupe CAPSEC ayant énormément travaillé sur les analyses des risques en laboratoires, les conditions nécessaires à leur réalisation et l'établissement d'indicateurs pour établir des questionnaires et évaluer les réponses.

Puis, la nécessité de deux journées de travail pleines s'est faite sentir. Nous avons associé à ces réunions des personnalités extérieures maitrisant bien le sujet afin de collecter leur expertise pour valider les orientations que nous prenions. Il s'agissait notamment de personnes du CNRS, de la DCSSI et du pôle SSI de du ministère de l'éducation nationale, situé dans l'académie d'Aix-Marseille.

Les académies étaient en train de réaliser un projet intéressant, sur lequel nous allions nous appuyer pour faire évoluer le notre : il s'agissait d'une étude de risques appliqué à un référentiel applicatif borné commun aux différents rectorats, ceci afin de rédiger une PSSI générique à laquelle les académies ajouteraient des règles spécifiques liées à leur applicatifs locaux.

Ce projet avait alors fait l'objet d'un appel d'offre et suivait son cours. La possibilité d'un mode opératoire similaire nous a semblé alors envisageable.

Dès lors, le travail du groupe avait trouvé sa forme définitive et ses travaux se sont orientés vers deux axes :

- Afin de pouvoir « évangéliser » les utilisateurs de leurs établissements respectifs et éventuellement les correspondants sécurité ou RSSI des établissements proches, les membres du groupe qui le désiraient ont suivi le stage de formateur EBIOS.
- Au fur et à mesure des connaissances accumulées et de l'expérience acquise aussi bien par nos collègues universitaires ayant des projets PSSI déjà avancés, que des collègues du scolaire dont le projet avançait ou encore le CNRS dont la PSSI était en cours de déclinaison dans un nombre restreint d'unités, nous avons pu rédiger un cahier des charges pour l'appel d'offres.

2 Les travaux

2.1 Méthodes d'élaboration d'une PSSI

2.1.1 Aider les établissements

Lorsqu'un établissement veut gérer la sécurité de son information et élaborer sa propre PSSI, il se retrouve devant un certain nombre d'actions à accomplir :

1.sensibiliser la direction et les responsables de structures internes à ces problématiques. Seuls les établissements ayant « souffert » (mauvaises expériences) ont pris la mesure des enjeux réels ;

2.assumer le coût humain et financier d'une démarche complète ;

3.disposer en interne des compétences appropriées pour mener à bien une démarche PSSI ;

4.choisir de façon pertinente une méthodologie qui correspond au contexte et aux moyens de l'établissement ;

Cette liste explique pourquoi un certain nombre d'établissements ne s'engagent pas plus loin dans cette direction.

Afin d'aider les établissements à s'engager dans une telle démarche de gestion de la sécurité de l'information, il faut leur proposer des solutions pour les aider à franchir ces obstacles.

On peut envisager trois méthodes pour atteindre cet objectif, ces méthodes conditionnant les outils que l'on va utiliser :

1.suivre la démarche préconisée dans un guide de bonnes pratiques et essayer de l'adapter à l'établissement;

2.réaliser une étude complète des risques encourus par les systèmes d'information de l'établissement afin de savoir quoi protéger contre qui et comment, et en déduire la PSSI.

3.l'aide à la mise en place d'un SMSI (Système de Management de la Sécurité de l'Information) dans chaque établissement ;

La première méthode a le mérite de prendre moins de temps pour la rédaction et d'être plus facile à mettre en œuvre à priori. Mais il y a un risque : dans le processus de choix des règles de sécurité, certaines peuvent-être choisies sans réel fondement. On forme ainsi un ensemble de vœux pieux qu'on stocke ensuite sur une étagère et qui finissent vite par être obsolètes car déconnectées de la réalité du terrain et des besoins réels.

2.1.2 Réaliser une étude de risques

La deuxième méthode permet de mieux coller aux besoins réels de sécurité, elle est systématique et se doit d'être exhaustive. Elle met en œuvre des méthodes d'analyse de risques développées et exploitées par des organismes reconnus dans le domaine de la sécurité. Ces méthodes sont souvent spécialisées dans des domaines particuliers (santé, industrie...). Les principes sont en général les suivants dans le cas des systèmes d'informations :

1.recenser de tous les biens importants en terme de sécurité de l'information (matériels, bâtiments, logiciels, personnels, savoir-faire, données, ...) ;

2.identifier les personnes responsables (« propriétaires ») de ces biens ;

3.recenser les vulnérabilités qui pèsent sur ces biens (fragilité de conception, mobilité du bien, trop grande visibilité, exposition aux conditions à risques .) ;

4.identifier les menaces (incendie ou dégâts des eaux, vol, abus de droit, actions illicites, espionnage) ;

5.identifier leurs impacts en terme d'intégrité, de confidentialité, de disponibilité ;

6.évaluer la vraisemblance de ces menaces en regard de l'environnement actuel des actifs ;

7.estimer les niveaux de risque.

Il ne « reste plus » qu'à savoir comment traiter le risque en spécifiant un certain nombre de mesures permettant de réduire, d'éviter, d'accepter ou de transférer ce risque. Réduire le risque signifie élaborer des mesures concrètes à appliquer.

L'ensemble des règles résultant des processus ci-dessus, constitue une PSSI.

2.1.3 Mettre en œuvre un SMSI

La mise en place d'un SMSI n'est pas la simple itération d'une méthode. Elle permet de s'assurer que la PSSI va bien être élaborée, qu'elle vit et qu'elle est mise à jour au fur et à mesure de la vie du système d'information de l'établissement (vulnérabilités découvertes, règles inadaptées aux usages.), et ce, entre autre grâce à des tableaux de bord. Outre la prise en compte de la vie du SI, cette méthode, conforme aux normes ISO2700x, permet de débuter avec peu d'éléments dans un premier passage d'appréciation du risque et d'affiner au fur et à mesure des révisions. En cela, elle est beaucoup plus souple. Néanmoins, pour des effets rapides, elle est plus lourde à mettre en place dans le sens où, l'adhésion de la direction n'est pas suffisante. C'est un véritable système de gestion dédié à la sécurité des informations qu'il faut mettre en place avec :

- des indicateurs;
- un comité de pilotage;
- un chef de projet.

Il s'agit :

1.d'établir des objectifs de sécurité relatifs à : la politique de sécurité, l'organisation de la sécurité, la gestion des actifs, la sécurité du personnel, la sécurité physique, la gestion de l'exploitation, le contrôle d'accès, le contrôle du changement, la gestion des incidents, la continuité de l'activité, la conformité,

2.d'évaluer la situation de la sécurité de l'information dans l'établissement,

3.d'établir une politique contenant des mesures techniques et organisationnelles afin d'atteindre les objectifs de sécurité,

4.de vérifier périodiquement si on atteint bien les objectifs et de corriger le cas échéant les règles afin de (au choix): atteindre ces objectifs, s'y maintenir, les dépasser.

La direction d'un établissement doit donc non seulement se sentir concernée par une telle organisation, mais elle doit aussi y prendre une part active.

2.1.4 Méthode sélectionnée

Nous avons estimé que l'étude de risque, malgré la lourdeur initiale de cette méthode possédait un certain nombre d'avantages indéniables, pour peu qu'elle soit réalisée par un cabinet d'audit. En effet, l'intervention d'une société extérieure permet d'établir un planning auquel il faut se tenir (de l'argent est en jeu). Le risque de voir le projet « glisser » dans le temps se retrouve ainsi limité. Tout vouloir réaliser en interne, crée le risque de voir les tâches quotidiennes prendre le dessus sur ce projet qui serait sans cesse retardé.

De plus, un tel audit ne se limite pas à quelques interviews de personnels stratégiques d'un établissement. La synthèse des ces interviews et leur concrétisation sous forme de règles doit être validée par la gouvernance. C'est surtout ici qu'il est intéressant de faire appel à une société extérieure :

- L'expertise reconnue de la société la fait passer pour crédible face aux personnes entretenues ;
- malgré toute l'expertise des membres du groupe de travail, l'étape de synthèse et de formalisation des règles est un exercice pour lequel ces sociétés sont parfaitement rodées.

Afin de réaliser ce travail et d'en tirer un bénéfice pour tous les établissements d'enseignement supérieur, il faut répondre aux questions suivantes :

- Quelles méthodes recommander pour réaliser les études de risque ?
- Comment allier les avantages d'un guide de bonne pratique et d'une étude de risques systématique dans chaque établissement voulant rédiger sa PSSI ?
- Si des études de risques sont réalisées par tous les établissements souhaitant rédiger une PSSI, comment mutualiser les résultats ?
- Comment accompagner chaque établissement s'engageant dans cette démarche afin qu'elle soit positive et durable ?

2.2 Bénéfices attendus de ce projet

Le groupe de travail GT-PSSI s'est prononcé sur un certain nombre d'éléments de réponse :

1.Suivant l'exemple des études PSSI en académies, il a projeté de mutualiser ces coûts en appliquant une étude de risques sur un nombre réduit d'établissements, suffisamment variés pour être représentatifs de notre communauté;

2.Les compétences ont été acquises au niveau du groupe de travail (expérience en établissement ainsi que formation) afin de pouvoir disséminer l'expertise au maximum;

3.Une méthode d'analyse de risques à été choisie : la méthode EBIOS de l'ANSSI avec la contrainte de l'utiliser en conformité avec la norme ISO27005

4.La mise en commun de ces études de risques doit permettre de dégager les points communs à tous les établissements et d'en déduire un certain nombre de règles, établissant ainsi ce que le groupe appelle une « PSSI générique »;

5.La PSSI générique sera accompagnée d'une boîte à outils permettant de l'adapter à tout autre établissement. Cette façon de procéder, rejoint ainsi la facilité apparente de la démarche « bonnes pratiques » en prenant en compte la réalité des environnements de l'enseignement supérieur et de la recherche et donc une plateforme réaliste de règles devant convenir à une certaine majorité d'établissements;

6.La démarche mise en œuvre doit s'accompagner d'un matériel de sensibilisation.

Au final, sept établissements ont décidé de participer au projet. Celui-ci devrait être réalisé par une société d'audit en coordination avec des équipes projet au sein de chaque établissement. Outre le fait que la réalisation de ces audits dans les sept établissements par une société extérieure permet potentiellement de tenir un planning précis, chaque établissement participant à l'opération aura le bénéfice de voir sa PSSI rédigée.

Une telle étude de risque réalisée à l'échelle d'un établissement peut être totalement illisible si on prend en compte toutes ses missions. Il parait illusoire de dégager des invariants communs à toutes les missions de tous les établissements audités. La PSSI générique pourrait se voir réduire à ce qu'on ne souhaite pas : juste un guide de bonnes pratiques.

C'est pourquoi, nous avons décidé de cloisonner cette PSSI en trois sous-parties correspondant aux missions que doit réaliser un établissement d'enseignement supérieur et aux fonctions transverses permettant de réaliser ces missions.

Ces trois périmètres sont :

- la formation;
- la recherche;
- la gestion;

La PSSI sera ainsi constituée d'une partie incontournable commune à tous les établissements, et de trois volets applicables séparément. L'effort de chaque établissement pour adapter cette PSSI à son propre contexte sera ainsi fractionné. De plus, pour le cas de la recherche par exemple, dans le cadre des UMR, l'articulation avec les PSSI des grands organismes de recherche (CNRS, INRIA, INSERM...) en sera facilitée, n'étant pas noyée dans l'ensemble des règles constituant la PSSI de l'établissement.

3 Le projet Retenu

3.1 Mode opératoire

Après s'être prononcé sur les points précédents, le groupe de travail s'est attelé à la rédaction d'un cahier des charges correspondant à la prestation souhaitée. La rédaction de ce CCTP n'a d'ailleurs pas été une mince affaire, car afin de s'assurer que les prestataires soumettant une offre aient bien compris le sujet, il fallait nous même retranscrire toutes nos préoccupations et bien faire saisir l'évolution de nos réflexions.

De plus, le souci de ne pas se limiter à une étude de risque qui verrait la rédaction d'une PSSI sans suite a pris de plus en plus d'importance et nécessitait d'être précisé dans ce cahier des charges.

Ce projet a pris l'aspect d'un groupement de commande entre les sept établissements concernés, l'appel d'offre étant lancé par l'Université de Rennes 1 (la cellule technique du CRU est hébergée dans ses locaux).

Cette prestation fait l'objet d'un lot unique mais comporte trois parties distinctes. En effet, pour que le projet soit un succès, il nous a semblé important que les études de risque des sept établissements soient réalisées simultanément afin de limiter la durée du projet. Ce parallélisme doit permettre à la société de service de disposer de toutes les données en même temps afin de les synthétiser.

Afin de réaliser cette condition sans multiplier le nombre d'intervenants du prestataire (et donc les coûts), ils nous a semblé judicieux que les interviews soient réalisées par une équipe projet dans chaque établissement. Pour avoir une grille commune lisible par le prestataire afin de synthétiser les réponses, il faut que ces équipes soient formées par ce prestataire et que les interlocuteurs au sein de l'établissement soient identifiés par ce même prestataire.

La prestation fait donc l'objet des phases suivantes :

- une phase de formation des équipes projet ;
- une phase d'entretiens réalisés par les équipes projet de chaque établissement ;
- une phase de collecte et de validation des résultats ;
- la rédaction de la PSSI générique ;
- le développement de la boîte à outils ;
- la validation de cette boîte à outil par la rédaction de la PSSI de chacun des sept établissements concernés.

Afin de donner la crédibilité nécessaire à cette PSSI dans l'établissement, la gouvernance est associée pour la validation des règles choisies pour cette PSSI. Un comité de pilotage dans chaque établissement sera donc associé au projet.

Afin de pouvoir faire des itérations ultérieures sur les études de risques, les bases de connaissances ainsi constituées lors des audits ainsi que la PSSI de chacun des sept établissements doivent être réutilisables et donc dans un format électronique exploitable.

Les livrables attendus sont les suivants :

- le résultat des études, les documents ayant servi à élaborer ces études EBIOS et bases de connaissances constituées et implémentées pendant l'analyse de risques (par domaine et par établissement). Tous ces éléments seront fournis sous la forme d'un document exploitable et de fichiers d'étude exploitables par un programme ou un tableur et accompagnés d'un outil permettant leur mise à jour lors d'itérations ultérieures de cette analyse.
- la PSSI générique accompagnée de tous les documents d'étape. Elle sera fournie au moins au format électronique (accompagné des sources du documents afin de faciliter les itérations dont elle fera l'objet lors de son adaptation).
- la boite à outil permettant d'adapter cette PSSI.
- les sept PSSI d'établissement.

La boîte à outil doit contenir les éléments suivants :

- un référentiel règlementaire ;
- une base de connaissances adaptée au contexte pour effectuer une étude de risques dont les livrables seraient conformes à la norme ISO27002 et tous les éléments nécessaires à l'analyse de risque ;
- les outils nécessaires aux entretiens utilisés par les équipes projets (supports de formation, guides d'entretiens, questionnaires types, fiches d'enquêtes…) ;
- une liste de besoins de sécurité, d'impacts et de règles qui n'auraient pas été retenus dans la PSSI générique avec la justification des choix (afin de permettre à un établissement voulant l'adapter de juger de la pertinence du retrait de cette règle vis à vis de sa situation) ;
- un guide de gestion de projet PSSI accompagné de questionnaires de sensibilisation à la sécurité ;
- un mode d'emploi qui indiquera les différentes manières de décliner la PSSI générique en fonction de cas types identifiés (multi-tutelles par exemple).

Afin que le projet ne soit pas sans suite dans les établissements, il nous a paru important d'y introduire des éléments des normes ISO2700x. Ainsi, la PSSI doit être rédigée en se basant sur la norme ISO27002 qui contient une liste de mesures liées à la sécurité du SI. De plus, afin d'introduire une dynamique SMSI, il nous a paru intéressant que, dans la boîte à outils figure :

- une grille de réutilisation des éléments de l'étude PSSI dans le cadre de la mise en place d'un SMSI (ISO 27001) ;
- un plan d'action pour la mise en œuvre des mesures de la PSSI (prenant en compte la hiérarchie des risques) ;
- une version de ce plan d'action comme base d'une DDA (déclaration d'applicabilité, cf. ISO27001) ;
- un plan d'action « type » (orienté gestion de projet) lié à notre environnement GESTION pour la mise en œuvre d'un SMSI ;
- un outil d'audit interne du SMSI pour mesurer nos écarts à l'ISO 27001.

Ainsi, pour le domaine qui constitue le quotidien des centres de ressources informatiques et de la gouvernance des établissements, les éléments d'une vie de la PSSI et de son évolution en phase avec la vie de l'établissement seront réunis.

3.2 Financement

Étant dans un cadre de mutualisation des moyens, il nous a paru intéressant de mobiliser le Ministère de tutelle sur cette opération. Il était prévu initialement qu'il participe à hauteur de la moitié des dépenses engagées sur ce projet. Le nombre

d'établissements initialement envisagé étant passé de cinq à sept, cette part a été légèrement réduite en proportion de l'apport de chaque établissement.

L'apport de chaque établissement participant au groupement de commande est fixe et a été fixé initialement par le groupe de travail en regard du budget évalué pour cette opération. Cet apport correspond au bénéfice qu'il en retire, c'est à dire :

- la formation d'une partie de son personnel à l'appréciation du risque ;
- la rédaction de sa PSSI par un prestataire spécialisé dans le domaine.

L'apport du Ministère correspond à la partie commune dont pourront bénéficier tous les établissements d'enseignement supérieur lorsque la PSSI générique et l'outillage nécessaire à son adaptation seront disponibles.

4 État du projet

Le projet a tout d'abord fait l'objet d'un appel d'offre en procédure adaptée. Les offres ont été évaluées au mois de juin 2009 et la commission a considéré l'appel d'offre comme étant infructueux, les sommes étant supérieures au plafond d'une procédure adaptée. L'appel d'offre a donc été relancé à la fin du mois d'août 2009. Le calendrier prévisionnel prévoit une notification des prestataires au début du mois de décembre 2009. Nous serons donc normalement en mesure d'annoncer le nom de la société et de produire un calendrier prévisionnel des actions. Celles-ci devraient néanmoins commencer en janvier et nous les avons évaluées sur une durée de sept mois environ.

Les sept établissements ayant pris part à l'appel d'offre doivent normalement être en possession de leur PSSI à la rentrée 2010-2011.

Bibliographie

[1] Nicole Dausque, Anne Facq, Gabrielle Feltin, Françoise Gazelle et Olivier Servas, article « Pourquoi et Comment Adapter une Politique de Sécurité pour les Entités du CNRS ? ». Dans *Actes du congrès JRES2005*, http://2005.jres.org/paper/112.pdf, Marseille, décembre 2005.

[2] ISO, Normes ISO 27001, 27002, 27005, http://www.iso.org/iso/fr/home.htm.

[3] Alexandre Fernandez-Toro. *Management de la sécurité de l'Information*. éd Eyrolles, Novembre 2007.

[4] ANSSI. *Outils méthodologiques de la SSI* (méthode EBIOS, PSSI, tableaux de bord SSI...) http://www.ssi.gouv.fr/site_rubrique41.html